OIG

Office of Inspector General

Semiannual Report to the Congress

October 1, 2018–March 31, 2019

FDIC

Federal Deposit Insurance Corporation

Under the Inspector General Act of 1978, as amended, the Federal Deposit Insurance Corporation Office of Inspector General (FDIC OIG) has oversight responsibility of the programs and operations of the FDIC.

The FDIC is an independent agency created by the Congress to maintain stability and confidence in the nation's banking system by insuring deposits, examining and supervising financial institutions, and managing receiverships. Approximately 5,700 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured more than $7.5 trillion in deposits in 5,406 institutions, of which the FDIC supervised 3,483. The Deposit Insurance Fund balance totaled $102.6 billion as of December 31, 2018. Active receiverships as of March 31, 2019, totaled 271, with assets in liquidation of about $1.04 billion.

Office of Inspector General

Office of Inspector General

Semiannual Report to the Congress

October 1, 2018–March 31, 2019

Federal Deposit Insurance Corporation

Inspector General's Statement

On behalf of the Office of Inspector General (OIG) at the Federal Deposit Insurance Corporation (FDIC), I am pleased to present the Semiannual Report for the period of October 1, 2018 through March 31, 2019. The work highlighted in this Report illustrates the broad range of our oversight responsibilities and the importance of our work for the agency, financial sector, policymakers, and the American people.

During the reporting period, we issued our Top Management and Performance Challenges document, which identified nine significant risks facing the FDIC. The FDIC faces Challenges in several critical areas:

- Enhancing Oversight of Banks' Cybersecurity Risk;
- Adapting to Financial Technology Innovation;
- Strengthening FDIC Information Security Management;
- Preparing for Crises;
- Maturing Enterprise Risk Management;
- Sharing Threat Information with Banks and Examiners;
- Managing Human Capital;
- Administering the Acquisitions Process; and
- Improving Measurement of Regulatory Costs and Benefits.

This assessment was based on our oversight work, extensive research, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private-sector entities.

In addition, we issued several Audit reports during this Semiannual Report period, including on the FDIC's Information Security Program; Controls over the FDIC's System Interconnections that enable the FDIC to exchange significant amounts of data with outside organizations; and a report that questioned costs related to contractor billings for application support services. These reports contained 24 important recommendations for improvement to the FDIC's operations and functions. We are closely monitoring the agency's progress in implementing these OIG recommendations and actions taken to address our recommendations.

In addition, the OIG conducted significant investigations into criminal and administrative matters involving complex multi-million-dollar schemes of bank fraud, embezzlement, money laundering, and other crimes committed by corporate executives and bank insiders. For example, one OIG investigation resulted in a jury conviction of the Chairman and Chief Executive Officer of an international pharmaceutical company whose criminal actions caused losses of more than $100 million to a large Puerto Rican bank and contributed to its failure. Another case involved a former political consultant and campaign manager for the President. We also investigated significant matters that led to successful outcomes against two FDIC employees. Our investigations during this period resulted in 26 convictions, as well as fines, restitution orders, and forfeitures over $219 million. In addition, our cases led to 15 arrests and 36 indictments and informations.

Also, as we issue this Semiannual Report, our OIG is celebrating its 30th Anniversary. I would like to recognize and commend the prior Inspectors General who preceded my tenure: Robert D. Hoffman, James A. Renick, Gaston L. Gianni, Jr., and Jon T. Rymer. Our Office has thrived under their leadership over the past three decades.

We appreciate the continued support of Members of the Congress and staff; the FDIC Chairman, Board, and other executive leaders; as well as our colleagues within the IG community. In addition, I am grateful for the hard work and dedication of the women and men of the OIG. We remain committed to serving the American people as a leader in the IG community.

Jay N. Lerner
Inspector General
April 30, 2019

Table of Contents

Acronyms and Abbreviations

AEB	American Enterprise Bank
C&C	Cotton & Company LLP
CEO	Chief Executive Officer
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIOO	Chief Information Officer Organization
CMI	Compensation Management Incorporated
CNB	Community National Bank
D&I	Diversity and Inclusiveness
DOA	Division of Administration
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOF	Division of Finance
DOJ	Department of Justice
EA	Enterprise Architecture
ERM	Enterprise Risk Management
FBAR	Foreign Bank and Financial Account

FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
GSB	Grand South Bank
IG	Inspector General
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
RMS	Division of Risk Management Supervision
SAR	Suspicious Activity Report
SBA	Small Business Administration
TMPC	Top Management and Performance Challenge
TVA	Tennessee Valley Authority
USAO	U.S. Attorney's Office

Introduction and Overall Results

The FDIC OIG mission is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency. Our vision is to serve the American people as a recognized leader in the Inspector General community: driving change and making a difference by prompting and encouraging improvements and efficiencies at the FDIC; and helping to preserve the integrity of the agency and the banking system, and protect depositors and financial consumers.

Our Office conducts its work in line with a set of Guiding Principles that we have adopted as One OIG, and the results of our work during the reporting period are presented in this report within the framework of those principles. Our Guiding Principles focus on impactful Audits and Evaluations; significant Investigations; partnerships with external stakeholders (the FDIC, Congress, whistleblowers, and our fellow OIGs); efforts to maximize use of resources; Leadership skills and abilities; and importantly, Teamwork.

30 Years: Making a Difference
FDIC OIG • 1989-2019

30 and Thriving

Our office has evolved from its earliest composition as a group of internal audit and investigative staff to an office now headed by a Presidentially appointed and Senate confirmed IG, comprised of a skilled staff of auditors, evaluators, attorneys, analysts, human resource specialists, IT professionals, and Federal law enforcement agents.

On March 14, 1989, an FDIC Board resolution recognized that the Inspector General Act Amendments of 1988 required the Corporation to establish an OIG with an IG who functions under the general supervision of the Chairman, and established that position as of April 17 of that year. The FDIC's former Office of Corporate Audits and Internal Investigations (OCAII) was re-designated the OIG. The Director of OCAII became Inspector General, and the incumbent Director, Robert D. Hoffman was designated Acting IG and then IG. Mr. Hoffman retired in 1993 and James A. Renick was selected by FDIC Acting Chairman Andrew "Skip" Hove to serve as IG.

In 1993, the Congress designated the IG position at the FDIC as a Presidential appointment, and Mr. Renick was named as Acting IG. On April 29, 1996, Gaston L. Gianni, Jr. became the FDIC's first IG appointed by the President. Jon Rymer was sworn in as the second Presidentially appointed IG on July 5, 2006, and resigned to become the Department of Defense IG on September 27, 2013. Fred W. Gibson, Jr. was named Acting IG following Mr. Rymer's departure and served in that capacity for 3½ years. On January 9, 2017, Jay N. Lerner was sworn in as the FDIC's third Presidentially appointed IG.

The following table presents overall statistical results from the reporting period.

Overall Results (October 1, 2018 – March 31, 2019)	
Audit, Evaluation, and Other Products Issued	7
Nonmonetary Recommendations	24
Investigations Opened	32
Investigations Closed	41
OIG Subpoenas Issued	9
Judicial Actions:	
Indictments/Informations	36
Convictions	26
Arrests	15
OIG Investigations Resulted in:	
Fines	$51,500
Restitution	$218,832,171*
Asset Forfeitures	$351,652
Total	$219,235,323
Referrals to the Department of Justice (U.S. Attorneys)	37
Proposed Regulations and Legislation Reviewed	2
Responses to Requests Under the Freedom of Information/Privacy Act	13

*Of this total amount, $37,088,621 was ordered joint and several with other individuals sentenced during this reporting period.

Audits, Evaluations, and Other Reviews

The FDIC OIG seeks to conduct superior, high-quality audits, evaluations, and reviews. We do so by:

- Performing audits, evaluations, and reviews in accordance with the highest professional standards and best practices.
- Issuing relevant, timely, and topical audits, evaluations, and reviews.
- Producing reports based on reliable evidence, sound analysis, logical reasoning, and critical thinking.
- Writing reports that are clear, compelling, thorough, precise, persuasive, concise, readable, and accessible to all readers.
- Making meaningful recommendations focused on outcome-oriented impact and cost savings.
- Following up on recommendations to ensure proper implementation.

We issued the results of four audits and two audit-related reviews during the reporting period, as summarized below. These reports contained 24 nonmonetary recommendations, questioned costs of $48,569, and focused in large part on information technology (IT) and cybersecurity issues. We also issued our Top Management and Performance Challenges document during the reporting period, highlighting nine areas of challenge for the FDIC.

Our office also reviews the failures of FDIC-supervised institutions causing material losses to the Deposit Insurance Fund. If the losses are less than the material loss threshold outlined in the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), we determine whether circumstances surrounding the failures would warrant further review. There have been no FDIC-supervised financial institution failures since October 13, 2017, and we conducted no such reviews during the reporting period, as noted in Appendix 2.

Federal Information Security Modernization Act (FISMA)

During the reporting period, we issued the results of our audit of the effectiveness of the FDIC's information security program and practices. The IG FISMA Reporting Metrics require IGs to assess the effectiveness of their agencies' information security programs and practices on a maturity model spectrum. We found that the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented) on a scale of 1 to 5, which is an improvement from 2017, but not considered effective under the metrics.

We found that the FDIC established a number of information security program controls and practices that complied or were consistent with standards and guidelines, and took steps to strengthen controls following the 2017 FISMA report. However, ongoing security control weaknesses limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. In many cases, these security control weaknesses were identified by other OIG audits or through security control assessments completed by the FDIC. Although the FDIC was working to address these previously identified control weaknesses, the FDIC had not yet completed corrective actions at the time of the audit. Accordingly, the security control weaknesses continued to pose risk to the FDIC. The highest risk weaknesses included:

Information Security Risk Management. The FDIC had not fully defined or implemented an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks, including those related to cybersecurity and the operation of information systems. This limits the ability of FDIC Divisions and Offices to make effective risk management decisions, and prevents the FDIC from ensuring it is effectively prioritizing resources toward addressing risks with the most significant potential impact on achieving strategic objectives.

Enterprise Security Architecture. Our 2017 FISMA audit noted that the FDIC had not established an enterprise security architecture, which is considered a fundamental component of an effective information security program and describes the structure and behavior of an organization's security processes, systems, personnel, and subunits and shows their alignment with the organization's mission and strategic plans. In July 2018, the FDIC provided the OIG with documentation describing its enterprise security architecture. The OIG is reviewing this documentation, along with other information related to the enterprise security architecture provided by the FDIC, to determine whether it is responsive to the recommendation in our FISMA audit report issued in 2017. The lack of effective enterprise security architecture increased the risk that the FDIC's information systems would be developed with inconsistent security controls that are costly to maintain.

Security Control Assessments. In separate OIG audit work, we identified instances in which contractor-performed security control assessments did not include testing of security control implementation, when warranted. Instead, assessors relied on narrative descriptions of the controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel. Without testing, assessors did not have a basis for concluding on the effectiveness of security controls. Inadequate FDIC oversight of security control assessments contributed to this weakness. Because the FDIC relies on the results of the assessments to support a number of important risk management activities, the FDIC must ensure that personnel perform security control assessments at an appropriate level of depth and coverage.

Patch Management. The FDIC's patch management processes were not always effective in ensuring that the FDIC implemented patches within FDIC-defined timeframes. Unpatched systems increase the risk of exposing the FDIC's network to a security incident.

Backup and Recovery. Our 2017 FISMA report noted that the FDIC's IT restoration capabilities were limited and that the FDIC had not taken timely action to address known limitations with respect to its ability to maintain or restore critical IT systems and applications during a disaster. In December 2017, the FDIC's Board of Directors authorized a multi-year Backup Data Center Migration Project to ensure that designated IT systems and applications supporting mission-essential functions can be recovered within targeted timeframes. While the FDIC established governance over this project, assurance that the FDIC can maintain and restore mission-essential functions during an emergency within applicable timeframes will be limited until the scheduled completion of the project in 2019.

We made four new recommendations to improve the effectiveness of the FDIC's information security program controls and practices.

Security Configuration Management of the Windows Server Operating System

We audited the FDIC's controls for managing security configurations and changes to its Microsoft Windows Server operating system. At the start of 2018, the FDIC had 2,166 servers on its network running the Microsoft Windows Server operating system. These servers store and process a significant volume of sensitive information and support mission-critical functions.

Federal agencies are required by statute to comply with certain system configuration requirements. Without effective configuration management, information systems may not operate properly, stop operating altogether, or become vulnerable to security threats. The objective of the audit was to determine whether the FDIC established and implemented controls for managing changes to its Windows Server operating system that were consistent with Federal requirements and guidelines.

The FDIC established various controls to manage changes to its Windows Server operating system, including an approved baseline configuration for the operating system; a system to track and report system changes; and a governance body to evaluate proposed changes. These controls were consistent with Federal requirements and applicable guidelines.

However, we found several deficiencies in the FDIC's management of security configurations for its Windows servers:

- The FDIC did not establish current policies and procedures for managing changes to the Windows Server operating system. Accordingly, we did not have sufficient criteria to fully assess the FDIC's implementation of configuration management controls.
- The FDIC hired a contractor firm to assess certain security controls, including configuration management controls, for which the FDIC had also assigned the firm duties related to design and/or execution. Tasking this firm with assessing the effectiveness of its own work affected the independence of such assessments.
- FDIC oversight activities were inadequate in identifying instances in which security control assessors did not perform actual testing of certain security controls, when appropriate, including those intended to protect the Windows Server operating system. In these cases, when concluding on control effectiveness, assessors relied solely on written descriptions of the controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel.
- The security plan for the Windows Server operating system contained several inaccurate descriptions of security controls.

Our report included eight recommendations collectively intended to ensure that (a) IT policies and procedures remain current and that personnel responsible for their implementation receive proper training; (b) security control assessments are performed by sufficiently independent entities; (c) oversight of security control assessments is sufficient and documented; and (d) system security plans remain accurate. The FDIC concurred with the recommendations. The FDIC already completed actions to address two of the recommendations, and plans to complete actions to address the remaining six recommendations by November 29, 2019.

Controls Over System Interconnections with Outside Organizations

We issued an audit report that focused on the FDIC's system interconnections, which enable the FDIC to exchange significant amounts of data with outside organizations. As of September 7, 2017, the FDIC had 11 system interconnections. The FDIC uses these system interconnections to transmit data, including personally identifiable information, confidential bank examination information, and sensitive financial data. Proper design of these interconnections is critical to reducing security risks such as unauthorized access or disclosure of agency information.

Our audit objective was to assess the FDIC's controls for managing system interconnections with outside organizations. The audit focused on key controls recommended by the National Institute of Standards and Technology (NIST) for managing system interconnections, such as written agreements that specify the technical and security safeguards needed to protect interconnections.

We found that:

- Although the FDIC issued certain policies, procedures and templates for establishing system interconnections, we identified control weaknesses in each of the four phases of the NIST life-cycle framework. The NIST framework consists of four phases: planning, establishing, maintaining, and terminating interconnections.
- The FDIC's policies and procedures did not: (a) define the types of technologies and configurations that constitute a system interconnection; (b) articulate the roles and responsibilities for those involved in managing system interconnections; or (c) establish documentation requirements for key activities.
- The FDIC did not create necessary written agreements to govern 3 of the 11 system interconnections.

- In four instances in which written agreements governing system interconnections had expired, the system interconnection remained enabled. In addition, the FDIC did not terminate three system interconnections when they were no longer needed.

We made seven recommendations to the FDIC to: (1) modify existing policies and procedures to address all four phases of the NIST life-cycle framework for managing system interconnections; (2) execute written agreements with two outside organizations; (3) modify the FDIC's standard contract language involving system interconnections to align with NIST guidance; (4) review system interconnection agreements annually to ensure that they remain current; (5) implement procedures to review, update, and reauthorize written agreements when appropriate; (6) develop and implement procedures for notifying technical staff when system interconnections are terminated; and (7) develop and implement policies and procedures to govern the secure transfer of data outside the FDIC when using technologies that are not considered system interconnections.

The FDIC concurred with six of the seven recommendations and partially concurred with the remaining recommendation. The FDIC provided an alternative corrective action to address the remaining recommendation.

Payments to Pragmatics, Inc.

We issued an audit report involving IT application support services that a contractor, Pragmatics, Inc., (Pragmatics) and an associated subcontractor provided to the FDIC. The FDIC relies extensively on contractors to maintain its portfolio of IT applications. These IT applications support mission-critical functions, such as the supervision of insured financial institutions and the resolution of failed financial institutions. Between May 2013 and March 2018, the FDIC spent nearly $192 million on IT application support services. As of March 1, 2018, the FDIC had awarded seven task orders to Pragmatics for such services, valued at $18.5 million.

The audit was conducted in response to a complaint received through the OIG Hotline. The complainant alleged that an employee working for a subcontractor of Pragmatics billed the FDIC for labor hours that the employee did not actually work. The complainant also alleged that Pragmatics and one of its subcontractors may have inappropriately billed contractor employee labor hours.

The objective of our audit was to determine whether certain labor charges paid to Pragmatics were adequately supported, allowable under the contract, and allocable to their respective task orders.

We questioned costs of approximately $47,500 (about 10 percent of the labor charges we reviewed), because they were either not adequately supported or unallowable:

- About $7,500 was unsupported because the employees who billed the hours did not access the FDIC's network or facilities on the days they charged the hours, and the nature of the work required access to the FDIC's network.
- The remaining amount of approximately $40,000 was unallowable because the work was performed off site (away from FDIC facilities). The FDIC's contract with Pragmatics required the contractor to perform all work at the FDIC's facilities, absent a site visit and approval by the FDIC to perform the work at an alternate location.

All of the labor charges we reviewed were properly allocated to their respective task orders.

Our report noted that FDIC personnel did not maintain documentation regarding the outcome of a site visit (July 2013), including whether the FDIC had approved Pragmatics personnel to work at the off-site location. Further, the FDIC did not identify the place of performance for services in the associated task orders.

We recommended that the FDIC determine the portion of the nearly $47,500 in unsupported or unallowable costs that should be disallowed and recovered; determine whether other labor charges billed by Pragmatics were unsupported and should be disallowed and recovered; document the results of the Pragmatics site visit and remind contracting personnel of the requirement to document such visits; and ensure that all contracts for IT application support services identify the place of performance. The FDIC expected to complete actions to address all seven of our recommendations by March 29, 2019.

Memorandum Reports Issued

Analysis of FDIC Purchase Card and Convenience Check Transactions. We conducted an analysis of the FDIC's Purchase Card and convenience check transactions to understand the associated risks and support our annual audit and evaluation planning. Our analysis identified concerns related to the payment of unnecessary credit card processing fees by the FDIC, the reporting of sales tax charges by merchants, and other issues. We discussed these concerns with Division of Administration (DOA) staff who had responsibility for managing and reviewing the Purchase Card Program. DOA had either taken or planned to take actions to address our concerns.

Loan Sample Methodology of Examinations. We issued a memorandum conveying the OIG's observations related to the FDIC's Loan Sample Selection Methodology for Examinations. In June 2016, we initiated an evaluation of the loan sample selection methodology, including examiner compliance with relevant guidance. We reviewed loan information for a judgmental sample of examinations performed at 16 FDIC-supervised institutions, and we analyzed loan sample information for FDIC examinations completed during 2015 through 2017. We completed certain aspects of our fieldwork and determined that it did not warrant further resources to continue the evaluation. Although we did not complete the evaluation in this area, we reported our observations, as we believed they provided useful insights on how examiners implement loan sampling during the examination process.

Top Management and Performance Challenges Facing the FDIC

Each year, Federal Inspectors General are required to identify and report on the top challenges facing their respective agencies, pursuant to the Reports Consolidation Act of 2000. During the reporting period, we issued our report, which identifies the Top Management and Performance Challenges (TMPC) facing the FDIC.

The OIG's TMPC report is based upon the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. We considered this body of information in light of the current operating environment and circumstances and our independent judgment.

We reported that the FDIC faces Challenges in several critical areas, a number of which remain from previous years:

- Enhancing Oversight of Banks' Cybersecurity Risk;
- Adapting to Financial Technology Innovation;
- Strengthening FDIC Information Security Management;
- Preparing for Crises;
- Maturing Enterprise Risk Management;
- Sharing Threat Information with Banks and Examiners;
- Managing Human Capital;
- Administering the Acquisitions Process; and
- Improving Measurement of Regulatory Costs and Benefits.

We believe that the FDIC should focus its attention on these Challenges, and we intended the document we issued to inform policymakers, including the FDIC and Congressional oversight bodies, and the American public about the programs and operations at the FDIC and the Challenges it faces. A brief summary of these challenges follows:

Enhancing Oversight of Banks' Cybersecurity Risk. Cybersecurity continues to be a critical risk facing the financial sector. Cyber risks can affect the safety and soundness of institutions and lead to the failure of banks, thus causing losses to the FDIC's Deposit Insurance Fund. For example, a cybersecurity incident could disrupt services at a bank, resulting in the exploitation of personal information in fraudulent or other illicit schemes, and an incident could start a contagion that spreads through established interconnected banking relationships. Despite increased spending on cybersecurity, banks are encountering difficulties in getting ahead of the increased frequency and sophistication of cyberattacks. The FDIC's IT examinations should ensure strong management practices within financial institutions and at their service providers.

Adapting to Financial Technology Innovation. FDIC policymakers and examiners must keep pace with the adoption of new financial technology to assess safety and soundness of institutions and its impact on the stability of the banking system. The pace of change and breadth of innovation requires that the FDIC create agile and nimble regulatory processes, so that it can respond to and adjust policies, examination processes, supervisory strategies, preparedness and readiness, and resolution approaches as needed.

Strengthening FDIC Information Security Management. The FDIC maintains thousands of terabytes of sensitive data within its IT systems and has more than 180 IT systems that collect, store, or process the personally identifiable information of FDIC employees; bank officials at FDIC-supervised institutions; and bank customers, depositors, and bank officials associated with failed banks. FDIC systems also hold sensitive supervisory data about the financial health of banks, bank resolution strategies, and resolution activities. The FDIC must continue to strengthen its implementation of governance and security controls around its IT systems to ensure that information is safeguarded properly.

Preparing for Crises. Central to the FDIC's mission is readiness to address crises in the banking system. The FDIC must be prepared for a broad range of crises that could impact the banking sector. These readiness activities should help to ensure the safety and soundness of institutions, as well as the stability and integrity of our nation's banking system.

Maturing Enterprise Risk Management. Enterprise Risk Management (ERM) is a critical part of an agency's governance, as it can inform prudent decision-making at an agency, including strategic planning, budget formulation, and capital investment. ERM program requirements include identifying risks that could affect the organization (Risk Profile and Inventory), establishing the amount of risk an organization is willing to accept (Risk Appetite), prioritizing strategies to address risks in the proper sequence, and responding to and mitigating the risks. The FDIC established an ERM program office in 2011, but has neither developed the underlying ERM program requirements nor realized the benefits of a mature ERM program.

Sharing Threat Information with Banks and Examiners. Federal Government agencies and private-sector entities share information about threats to U.S. critical infrastructure sectors, including the financial sector. Sharing actionable and relevant threat information among Federal and private-sector participants protects the financial system by building threat awareness and allowing for informed decision-making. The FDIC must ensure that relevant threat information is shared with its supervised institutions and FDIC examiners as needed, in a timely manner, so that actions can be taken to address the threats. Threat information also provides FDIC examiners with context to evaluate banks' processes for risk identification and mitigation strategies.

Managing Human Capital. The FDIC relies on skilled personnel to fulfill its mission, and 68 percent of the FDIC's operating budget for 2019 ($1.8 billion) was for salaries and associated benefits for employees. Forty-two percent of FDIC employees are eligible to retire within 5 years, which may lead to knowledge and leadership gaps. To ensure mission readiness, the FDIC should find ways to manage this impending shortfall. In addition, the FDIC should seek to hire individuals with the advanced technical skills needed for IT examinations and supervision of large and complex banks.

Administering the Acquisitions Process. The FDIC relies heavily on contractors for support of its mission, especially for IT and administrative support services. The average annual expenditure by the FDIC for contractor services over the past 5 years has been approximately $587 million. The FDIC should maintain effective controls to ensure proper oversight and management of such contracts and should conduct regular reviews of contractors. In addition, the FDIC should perform due diligence to mitigate security risks associated with supply chains for goods and services.

Improving Measurement of Regulatory Costs and Benefits. Before issuing a rule, the FDIC should ensure that the benefits accrued from a regulation justify the costs imposed. The FDIC should establish a sound mechanism to measure both costs and benefits at the time of promulgation, and it should continue to evaluate the costs and benefits of a regulation on a regular basis, even after it has been issued.

****

Ongoing audit and evaluation reviews at the end of the reporting period were addressing such issues as the FDIC's controls for preventing and detecting cyber threats, physical security risk management program, contract oversight management, Minority Depository Institution Program, Anti-Sexual Harassment Program, and readiness for the next crisis, among others. These ongoing reviews are also listed on our Website and, when completed, their results will be presented in an upcoming semiannual report.

CIGFO Issues Top Management and Performance Challenges Facing Financial Regulatory Organizations

In late September, the Council of Inspectors General on Financial Oversight (CIGFO) issued a report that presents The Top Management and Performance Challenges Facing Financial Regulatory Organizations. The joint report identified the following cross-cutting challenges affecting the financial regulatory sector, many of which align with those we identified at the FDIC:

- Enhancing Oversight of Financial Institution Cybersecurity;
- Managing and Securing Information Technology at Regulatory Organizations;
- Sharing Threat Information;
- Readiness for Crises;
- Strengthening Agency Governance; and
- Managing Human Capital.

The report highlights the importance of government-wide coordination and information sharing – in a whole-of-government approach, as distinct from considering the issues on an agency-by-agency basis. It also is a demonstration of the value and importance of OIGs working together to address critical cross-cutting issues facing the U.S. Government.

Investigations

The FDIC OIG investigates significant matters of wrongdoing and misconduct relating to FDIC employees, contractors, and institutions. We do so by:

- Conducting thorough investigations consistent with the highest professional standards and best practices.
- Working on important and relevant cases that have the greatest impact.
- Building and maintaining relations with FDIC and law enforcement partners to be involved in leading banking cases.
- Enhancing information flow to proactively identify law enforcement initiatives and cases.
- Recognizing and adapting to emerging trends in the financial sector.
- Developing expertise to shape the character of the OIG's investigative component and its Field Offices.

Our investigations are largely based upon referrals from the FDIC; our law enforcement partners, including other Offices of Inspector General; and the Department of Justice (DOJ), including U.S. Attorneys' Offices (USAO) and the Federal Bureau of Investigation (FBI). Our Office plays a key role in investigating sophisticated schemes of bank fraud, money laundering, embezzlement, and currency exchange rate manipulation. Our cases often involve bank executives, officers, and directors; other financial insiders such as attorneys, accountants, and commercial investors; private citizens conducting businesses; and in some instances, FDIC employees. A recent area of focus for our investigations has been partnering with other regulatory agencies to identify fraud in the guaranteed loan portfolios of FDIC-supervised banks. Such fraud schemes can affect the financial condition of banks and the financial services industry.

The cases discussed below are illustrative of some of the OIG's investigative success during the reporting period. They are the result of efforts by FDIC Special Agents in Headquarters, Regional Offices, and the OIG's Electronic Crimes Unit. As noted, these cases reflect the cooperative efforts of OIG investigators, FDIC Divisions and Offices, other OIGs, USAOs, and others in the law enforcement community throughout the country. These working partnerships contribute to ensuring the continued safety and soundness of the nation's banks and help ensure integrity in the FDIC's programs and activities.

South Florida Resident Convicted of a $100 Million International Fraud Scheme That Led to the Collapse of One of Puerto Rico's Largest Banks

On February 4, 2019, a Key Biscayne, Florida resident was convicted of eight counts of wire fraud affecting a financial institution after a 3-week trial in the Southern District of Florida. His scheme triggered a series of events leading to the insolvency and collapse of Westernbank of Puerto Rico.

According to evidence presented at trial, from 2005 to 2007, the South Florida resident served as chairman and chief executive officer (CEO) of Inyx, Inc., a publicly-traded multinational pharmaceutical manufacturing company. Beginning in early 2005, he caused Westernbank to enter into a series of loan agreements in exchange for a security interest in Inyx's assets. Under the loan agreements, Westernbank agreed to advance money based on Inyx's customer invoices from "actual and bona fide" sales.

However, the chairman and CEO orchestrated a scheme to defraud Westernbank by causing numerous Inyx employees to make tens of millions of dollars' worth of fake customer invoices purportedly payable by customers in the United Kingdom, Sweden, and elsewhere. He caused these invoices to be presented to Westernbank as valid invoices and made false representations to Westernbank about purported repayments from lenders in order to lull Westernbank into continuing to lend money to Inyx. He also fraudulently represented to Westernbank executives that he had additional collateral, including purported mines in Mexico and Canada worth hundreds of millions of dollars, to induce Westernbank to lend additional funds.

The chairman and CEO caused Westernbank to lend approximately $142 million and diverted tens of millions of dollars for his own personal benefit, including to buy a private jet, luxury homes and cars, luxury hotel stays, and extravagant jewelry and clothing expenditures.

In or around June 2007, Westernbank declared the loan in default and ultimately suffered losses exceeding $100 million. These losses later triggered a series of events leading to Westernbank's insolvency and ultimate collapse. At the time of its collapse, Westernbank had approximately 1,500 employees and was one of the largest banks in Puerto Rico.

In addition, the chairman and CEO knowingly deposited a $3 million check at Mellon Bank from the purported sale of his private jet. At the time of its deposit, he knew that the check was worthless – he had actually agreed to sell his plane to a different buyer. After receiving a provisional credit for the check from Mellon Bank, he wired out all of the provisional credit, including a $1 million wire to his personal account in Canada. Upon Mellon Bank's request to reverse this $1 million wire, the chairman and CEO refused to do so, resulting in at least a $1 million loss to Mellon Bank.

Source: *The FDIC's Division of Resolutions and Receiverships.*
Responsible Agencies: *FDIC OIG. Prosecuted by the U.S. Attorney's Office, Southern District of Florida.*

Former Bank President Sentenced to Prison and Ordered to Pay $137 Million

On December 14, 2018, the former president and CEO of The Bank of Union in El Reno, Oklahoma, was sentenced to 4 years in federal prison followed by 2 years of supervised release for making a false statement to the FDIC. He had previously pleaded guilty to this charge in 2017. The sentence requires the former president to pay over $137 million in restitution, over $97 million of which is owed to the FDIC. State banking regulators closed The Bank of Union in 2014 because of the bank's loan losses, and the FDIC was appointed as receiver.

According to a 2016 indictment, the former president defrauded the bank in several ways: (1) issuing loans with insufficient collateral and falsifying financial statements for several high-dollar bank borrowers; (2) originating nominee loans to circumvent the bank's legal lending limit; (3) concealing the bank's true financial condition from the Board of Directors; (4) soliciting a fraudulent investment; and (5) falsely representing the bank's true status to the FDIC.

Over a 4-year period, the former president conspired with borrowers by issuing them millions of dollars in loans secured by collateral they did not have and issuing them new loans to keep them off of overdraft reports. The former president misled the bank's Board of Directors by falsely stating the borrowers were paying down their loans.

The former president also defrauded a partial owner and investor in the bank by convincing him to wire nearly $40 million. The former president falsely represented to the investor that the bank was growing rapidly and performing well and that his investment would not be at risk, despite knowing that the bank was on the brink of failure and needed an immediate capital infusion.

Finally, the former president was charged with falsely representing the bank's loan status to the FDIC. Between September 2012 and September 2013, he continued to renew certain unpaid loans by capitalizing unpaid interest. Pursuant to a 2013 FDIC examination, he allegedly falsely represented that he had not renewed or extended any loans without full collection of the interest due during that time period. He also falsely represented in writing that the bank had total equity capital of more than $36 million in July 2013, when he knew the bank's equity capital was significantly less.

The partial owner who wired money for the bank's benefit is due $40 million of the restitution amount, and the remaining $97 million is due to the FDIC, which lost money when it assumed the bank's liabilities as receiver in January 2014.

Source: *The FDIC's Division of Risk Management Supervision (RMS).*
Responsible Agencies: *FDIC OIG and the FBI. Prosecuted by the U.S. Attorney's Office, Western District of Oklahoma.*

Former Political Consultant and Presidential Campaign Manager Sentenced

On March 7, 2019, a former political consultant and presidential campaign manager was sentenced after being found guilty during a jury trial of two counts of bank fraud, five counts of tax fraud, and one count of failing to file reports of Foreign Bank and Financial Accounts (FBAR). The trial took place in the U.S. District Court, Eastern District of Virginia. He was sentenced to 47 months of imprisonment, 36 months of supervised release, restitution of a potential range of approximately $6-$25 million, and a $50,000 fine.

About a week later, on March 13, 2019, the former political consultant and presidential campaign manager was sentenced after pleading guilty in the District of Columbia to one count of conspiring against the United States (which includes a conspiracy to commit money laundering, tax fraud, failure to file FBARs, and violations of the Foreign Agents Registration Act) and one count of conspiring to obstruct justice (witness tampering). He was sentenced to 73 months of incarceration with 43 months to be served consecutively to the sentence previously imposed by the U.S. District Court for the Eastern District of Virginia. In addition, he was ordered to pay restitution in the amount of $6,164,032.

Between 2006 through 2015, the former consultant and his business partner acted as unregistered agents of a foreign government and foreign political parties. Specifically, they represented the Government of Ukraine, the President of Ukraine (Victor Yanukovych, who was President from 2010 to 2014), the Party of Regions (a Ukrainian political party led by Yanukovych), and the Opposition Bloc (a successor to the Party of Regions after Yanukovych fled to Russia). As a result of their Ukraine work, the two generated tens of millions of dollars in income which they hid and laundered through scores of United States and foreign corporations, partnerships, and bank accounts. Furthermore, they funneled this money through various foreign nominee companies and bank accounts, opened by them and their accomplices in nominee names and in various countries to include Cyprus, Saint Vincent, Grenadines, and the Seychelles. The two hid the existence and ownership of the foreign companies and bank accounts, falsely and repeatedly reporting to their tax preparers and to the United States that they had no foreign bank accounts. The former political consultant used his hidden overseas wealth to enjoy a lavish lifestyle in the United States, without paying taxes on that income. He used the offshore accounts to purchase multi-million dollar properties in the United States.

Between approximately 2015 and at least January 2017, when the Ukraine income dwindled after Yanukovych fled to Russia, the former consultant, with the assistance of his business partner, extracted money from the former consultant's United States real estate by, among other things, using those properties as collateral to obtain loans from multiple financial institutions. The two fraudulently secured more than $20 million in loans by falsely inflating the former consultant's and his company's income and by failing to disclose existing debt in order to qualify for the loans.

Source: *United States Department of Justice, Money Laundering and Asset Recovery Section.*
Responsible Agencies: *FDIC OIG, FBI, and Internal Revenue Service (IRS)-Criminal Investigation Division (CID). Prosecuted by the Special Counsel's Office of the U.S. Department of Justice.*

Former Bank Vice President/Manager Sentenced to 15 Months in Prison

On November 20, 2018, a former bank vice president was sentenced to 15 months in prision, 36 months of supervised release, and ordered to pay $7.5 million in restitution. He previously pleaded guilty to one count of conspiracy to commit fraud against the United States for his involvement in a multi-million dollar nominee lending and tax fraud scheme that put significant strain on the capital reserve of Grand South Bank (GSB).

A Greensboro businessman operated several businesses, including Compensation Management Incorporated (CMI), which was a staffing company that recruited and employed temporary employees, called clients, to fill termed positions with various companies in the Greensboro area. To fund their monthly operations and payroll, the businessman entered into a factoring agreement with GSB, using CMI as the beneficiary. As a part of the factoring agreement, GSB would provide short-term loans (advances) to CMI to fund payroll and other business operating expenses until the staffing company received payment on the invoices issued to its clients for staffing services. Advances were collateralized by these invoices, also called accounts receivable. In addition to the short-term business loans, GSB had also made personal loans to the businessman in excess of $1 million. The former banker was the vice president and manager of the factoring department as well as the businessman's loan officer.

In or about 2008 and after, the banker advised the businessman that GSB had reached its legal lending limit and that any additional loans made to him would over-expose the bank, violate state banking laws, and attract scrutiny by the federal and state regulators. As a result, the businessman and the banker, with the aid of others, conspired to create five shell recruiting companies that acted as nominee borrowers for the businessman's expanding staffing business. The banker, aided by his assistant, created official bank records listing the five companies as separate entities owned by individual borrowers, when in fact all monies flowed through to the one businessman. The banker also helped to facilitate the withholding of payroll taxes from the salaries of staffing employees. These payroll funds were never submitted to the government but instead retained by GSB and in part converted to the businessman's personal use. The banker continued to advance additional funds to the businessman with knowledge of these unpaid payroll taxes. The aggregate of all fraudulent transactions totaled approximately $10.4 million.

Source: *U.S. Attorney's Office, Middle District of North Carolina, and the IRS.*
Responsible Agencies: *FDIC OIG, FBI, and IRS-CID. Prosecuted by the U.S. Attorney's Office, Middle District of North Carolina.*

Green Bay Businessman Sentenced in Securities Fraud Scheme

On January 23, 2019, a Green Bay, Wisconsin, businessman was sentenced to 90 months in prison, 3 years of supervised release, and ordered to pay $9,428,618 in restitution for his role in orchestrating a securities fraud scheme. On October 10, 2018, he pleaded guilty to one count of wire fraud. He was previously indicted on September 19, 2017 on 10 counts of wire fraud and 4 counts of money laundering. The businessman's two co-conspirators pleaded guilty to conspiracy to commit wire fraud on October 22, 2018, and January 10, 2019, respectively.

The indictment describes how, between March 2011 and August 2015, the businessman defrauded lenders and investors with his "Green Box" business plan. He promoted Green Box as an environmentally friendly recycling operation that would convert waste entirely into paper products and energy, without creating any waste-water discharge or landfill byproducts. He obtained approximately $9.4 million under false representations that investor funds would be used for the "Green Box" business plan. In reality, the businessman used most of those funds for personal expenditures, payment of unrelated debts, and efforts to further promote his scheme. The victims included the Wisconsin Economic Development Corporation, foreign investors who made investments through the United States Citizenship and Immigration Services EB-5 program, Cliffton Equities, and several local investors.

In a separate but related investigation, the businessman, his wife, and a Horicon Bank loan officer were indicted on April 16, 2016, on a series of criminal charges that included bank fraud and conspiracy. The businessman and the loan officer eventually pleaded guilty to their roles in the conspiracy; the charges against the businessman's wife were dropped.

Source: *The Brown County (Wisconsin) Sheriff's Department.*
Responsible Agencies: *FDIC OIG and the FBI. Prosecuted by the U.S. Attorney's Office, Eastern District of Wisconsin.*

Settlement Attorney Sentenced in Mortgage Fraud Scheme

On January 17, 2019, a disbarred attorney was sentenced to 41 months of imprisonment, followed by 5 years of supervised release. He was also ordered to pay restitution in the amount of $997,500, which is to be paid jointly and severally with his co-defendants.

In November 2016, Total Bank provided information alleging potential fraud with the acquisition of a duplicate residential mortgage loan acquired by a Colombian national citizen. An investigation revealed that the Colombian citizen's $2 million residential mortgage was one of six fraudulent loans created by a team of current and former real estate industry professionals, including the attorney, who worked together to acquire fraudulent loans in excess of $6 million. The co-defendants in this matter created fraudulent title companies to close on properties that were already encumbered. The fraudsters gained access to the properties through various individuals who were compensated or promised compensation for allowing them into the properties for the purpose of accommodating real estate appraisals that the lending institutions had ordered. The lending institutions involved were also provided fraudulent documentation regarding assets, income, employment and all other aspects of the loan acquisition process. The co-defendants assisted in the facilitation of loan closings but failed to record the transaction with county officials, while receiving incoming wires from the bank. Straw-purchasers such as the Colombian citizen were used to acquire loans based upon their credit, although the information provided on the loan applications was false.

Responsible Agencies: *FDIC OIG and the FBI. Prosecuted by the U.S. Attorney's Office, Southern District of Florida.*

Illinois Public Official Sentenced to 42 Months in Prison for Mail and Wire Fraud Scheme

On January 11, 2019, the former executive director of the Kankakee Valley Park District and former treasurer of a related not-for-profit foundation was sentenced to 42 months of imprisonment followed by 2 years of supervised release for mail fraud and wire fraud.

The public official previously pleaded guilty to using park district equipment, labor, funds, and other park district and foundation resources to build and maintain a pond on his personal property. He admitted that he converted park district and foundation funds intended for park district annual events for his personal use, and he used the park district's credit card to make unauthorized personal purchases. He also obtained a loan in the name of a non-existent foundation from an Illinois bank to fund some of the aforementioned projects. He failed to repay the loan.

Source: *Illinois State Police.*
Responsible Agencies: *FDIC OIG, FBI, and Illinois State Police. Prosecuted by the U.S. Attorney's Office, Central District of Illinois.*

Former Businessman Sentenced for Bank Fraud

On December 10, 2018, the former owner of ASK Industries, Inc., was sentenced in connection with his prior guilty plea to defrauding Community National Bank (CNB), N.A., Midland, Texas, an institution regulated by the Office of the Comptroller of the Currency. He was sentenced to serve 30 months in prison to be followed by 4 years of supervised release and ordered to pay restitution of $1,312,157 to CNB.

CNB operates the Capital Advantage Program, through which it issues lines of credit to small businesses to advance working capital against their accounts receivable. In 2010, CNB extended a line of credit to ASK Industries, Inc. and purchased approximately $60 million in invoices over a 5-year period. In November and December 2014, CNB unknowingly purchased 17 fraudulent invoices totaling approximately $1.4 million that the former owner of ASK Industries had submitted. ASK Industries defaulted on the line of credit in January 2014, and CNB ultimately lost $1.57 million on the line of credit.

Responsible Agencies: *FDIC OIG and the FBI. Prosecuted by the U.S. Attorney's Office, Western District of Texas.*

Bank Employees Sentenced for Teller Theft

On March 5, 2019, a former head teller was sentenced to 41 months of incarceration, 5 years of supervised release, and ordered to pay $1.66 million in restitution, jointly and severally with a former assistant teller. The assistant teller was sentenced to 21 months of incarceration, 5 years of supervised release, and ordered to pay $1.66 million in restitution, jointly and severally with the head teller.

On March 13, 2018 the two were indicted by a federal grand jury in the Middle District of Georgia. According to the indictment, they were charged with one count of conspiracy to defraud a financial institution, one count of false entries in bank records, and 23 counts of theft by a bank employee. On December 4, 2018, the two pleaded guilty to one count of conspiracy to defraud a financial institution. The additional charges were dismissed as part of their plea agreements.

The bank tellers used their positions of trust starting sometime during 2012 or 2013 to embezzle and misapply bank money by transferring bank funds into their personal bank accounts or into the accounts of family members and associates. The tellers took cash from their teller drawers and, in the head teller's case, directly from the vault. They also issued cashier's checks for their benefit, all without valid checks or cash being deposited in the bank to support these transactions. Between April 30, 2014 and March 14, 2016, the two were estimated to have stolen $1.66 million.

Source: *The FDIC's RMS.*
Responsible Agencies: *FDIC OIG and the FBI. Prosecuted by the U.S. Attorney's Office, Middle District of Georgia.*

Multiple Sentencings Completed in Loan Fraud Scheme

Multiple perpetrators of a complex loan scheme involving the sale and purchase of gas stations were sentenced during the reporting period:

- On January 4, 2019, a former loan officer for American Enterprise Bank (AEB) was sentenced to 36 months of imprisonment and 36 months of supervised released. He previously pleaded guilty to one count of bank fraud.
- On December 14, 2018, an individual who prepared false income tax returns in support of the loan fraud scheme was sentenced to one year and one day of imprisonment, 36 months of supervised released, and ordered to pay a special assessment of $100. He previously pleaded guilty to one count of bank fraud.

- On December 13, 2018, a former gas station broker who obtained Small Business Administration (SBA) loans through AEB, was sentenced to 36 months of imprisonment and 36 months of supervised release. He previously pleaded guilty to one count of bank fraud.

- On December 12, 2018, another former gas station broker who worked with the first broker to obtain SBA loans through AEB was sentenced to 66 months of imprisonment and 36 months of supervised release. He previously pleaded guilty to one count of bank fraud and one count of filing false federal tax returns.

Restitution for all defendants was to be determined at a hearing scheduled for April 4, 2019.

In late 2007, AEB approved eight SBA loans that one of the brokers used to purchase distressed Kum and Go brand gas stations. The broker made no improvements to the distressed properties and, shortly after taking ownership, conspired with others to sell these gas stations to uncreditworthy borrowers. These borrowers were recruited from the friends and extended families of the broker's co-conspirators and, with the other broker's assistance, the two purchased the gas stations with SBA-guaranteed loans, also from AEB. The loan officer approved loans totaling about $13,346,198. The broker and his co-conspirators caused false information, regarding the borrower's employment, income, assets, and liabilities to be submitted to AEB. The values of the distressed gas stations were also artificially inflated with the help of fraudulent appraisals, allowing the broker and his co-conspirators to realize significant profits. When the purchasers of these gas stations did not make the loan payments, AEB was forced to foreclose on properties that had very little value.

Source: *The FBI and SBA OIG.*
Responsible Agencies: *FDIC OIG, SBA OIG, FBI, and IRS-CID.*
Prosecuted by the U.S. Attorney's Office, Northern District of Illinois.

Vallejo Business Owner Sentenced for Multimillion Dollar Mortgage and Foreclosure Rescue Fraud Scheme

On November 2, 2018, a California business owner was sentenced to 14 years in prison for conspiring to commit wire fraud affecting a financial institution and bank fraud.

From about September 2004 through February 2008, the business owner and two co-conspirators operated Capital Access LLC, an entity in Vallejo. They preyed on homeowners nearing foreclosure, convinced them to sign away title in their homes, spent any equity those homeowners had saved, and used straw buyers to defraud federally insured financial institutions out of millions of dollars in home loans obtained under false pretenses. The equity that was taken from homeowners was then used for operational expenses of the scheme and personal expenses of the businessman and his co-conspirators.

As a result of the scheme, vulnerable homeowners across California lost their homes and savings, and lenders lost an estimated $10.47 million from the fraud.

Source: *FBI, Sacramento Field Office.*
Responsible Agencies: *FDIC OIG, FBI, and U.S. Postal Inspection Service. Prosecuted by the U.S. Attorney's Office, Eastern District of California.*

FDIC EMPLOYEE CASES

Although generally not a major focus of our investigative workload, the FDIC OIG conducts investigations of employee misconduct, and during the reporting period, our Office pursued two such cases, as described below.

Former Senior Employee at the FDIC Convicted of Embezzling Confidential Documents

On December 11, 2018, a former FDIC employee was found guilty before a federal jury in Brooklyn on both counts of an indictment charging her with theft of government property in the possession of the FDIC.

The senior employee worked in the FDIC's Office of Complex Financial Institutions in New York. In August of 2015, she used her office computer to review listings for and apply for jobs with financial institutions that filed living wills with the FDIC. On August 27, 2015, one day after being contacted about a possible position at one of the banks, she logged on to a secure FDIC database and printed out living will information for that institution. On September 16, 2015, the senior employee resigned from the FDIC, and data loss prevention software revealed that on her last day of work, she copied numerous electronic files from the FDIC network to external USB drives, including living wills for U.S. banks where she had been seeking employment.

Source: *The FDIC's Division of Information Technology.*
Responsible Agencies: *FDIC OIG. Prosecuted by the U.S. Attorney's Office, Eastern District of New York.*

Former FDIC IT Bank Examiner Sentenced for Filing False Claims

On November 7, 2018, a former FDIC IT bank examiner was sentenced to 5 months of incarceration, 80 hours of community service, 12 months of supervised release, and ordered to pay $65,567 in restitution to the FDIC for his role in submitting false travel claims to the FDIC. In December 2016, the former examiner was removed from Federal service with the FDIC.

The former examiner was employed by the FDIC in 2007 and later was promoted to an FDIC IT bank examiner. He participated in FDIC examinations of financial institutions that were located in numerous states. The FDIC also paid for him to attend training and conferences located in other states. Most examinations and training spanned multiple days. The FDIC authorized the former examiner to travel to the financial institutions and training, and incur travel expenses to stay overnight in nearby hotels, and incur other expenses, such as for car rental, for which the FDIC would reimburse him.

Between September 2012 and February 2016, the former examiner submitted multiple false and fraudulent claims for reimbursement, referred to as expense reports, using the FDIC's electronic travel voucher system. Each of these claims sought reimbursement for, among other things, hotel and/or car rental expenses that he did not incur. During the course of routine audits of these claims, the FDIC asked him to submit receipts supporting the claimed travel expenses. He submitted false and fraudulent receipts purporting to support the expenses that he had claimed. These receipts were created, or manufactured, for submission to the FDIC to support his prior false and fraudulent claims for reimbursement.

As an example, on January 29, 2016, the former examiner submitted to the FDIC a claim for reimbursement of travel expenses for the period covering January 11, 2016, through January 22, 2016, in the total amount of $3,705.62. Among other expenses, he claimed to have incurred $1,334.87 and $423.55 in hotel and rental car expenses, respectively, knowing that the claim was false, fictitious, and fraudulent.

Source: *The FDIC's Division of Finance and the FDIC's RMS.*
Responsible Agencies: *FDIC OIG. Prosecuted by the U.S. Attorney's Office, Northern District of Georgia.*

Strong Partnerships with Law Enforcement Colleagues

The OIG has partnered with various U.S. Attorneys' Offices throughout the country in bringing to justice individuals who have defrauded the FDIC or financial institutions within the jurisdiction of the FDIC, or criminally impeded the FDIC's examination and resolution processes. The alliances with the U.S. Attorneys' Offices have yielded positive results during this reporting period. Our strong partnership has evolved from years of hard work in pursuing offenders through parallel criminal and civil remedies resulting in major successes, with harsh sanctions for the offenders. Our collective efforts have served as a deterrent to others contemplating criminal activity and helped maintain the public's confidence in the nation's financial system.

During the reporting period, we partnered with U.S. Attorneys' Offices in the following areas: Alabama, Arkansas, California, Colorado, District of Columbia, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Puerto Rico.

We also worked closely with the Department of Justice; FBI; other OIGs; other Federal, state, and local law enforcement agencies; and FDIC Divisions and Offices as we conducted our work during the reporting period.

Keeping Current with Criminal Activities Nationwide

The FDIC OIG participates in the following bank fraud, mortgage fraud, cyber fraud, and other working groups and task forces throughout the country. We benefit from the perspectives, experience, and expertise of all parties involved in combating criminal activity and fraudulent schemes nationwide.

New York Region	Financial Fraud Enforcement Task Force; New York State Mortgage Fraud Working Group; New York Identity Theft Task Force; Newark Suspicious Activity Report (SAR) Review Task Force; Philadelphia SAR Review Team; El Dorado Task Force - New York/New Jersey High Intensity Drug Trafficking Area; South Jersey Bankers Association; Eastern District of New York SAR Meeting Group; New York External Fraud Group; Philadelphia Financial Exploitation Prevention Task Force; Bergen County New Jersey Financial Crimes Association; Long Island Fraud and Forgery Association; Connecticut USAO BSA Working Group; Connecticut U.S. Secret Service Financial Crimes Task Force; South Jersey SAR Task Force; Pennsylvania Electronic Crimes Task Force; National Crime Prevention Council, Philadelphia Chapter; Northern Virginia Financial Initiative SAR Review Team; Maryland Association for Bank Security; International Association of Financial Crimes Investigators.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force; Richmond Tidewater Financial Crimes Task Force.
Kansas City Region	Minnesota Inspector General Council; Minnesota Financial Crimes Task Force; Kansas City SAR Review Team; Nebraska SAR Review Team.
Chicago Region	Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Central District of Illinois Financial Fraud Working Group; Northern District of Illinois SAR Review Team; Southern District of Illinois SAR Review Team; Northern District of Illinois Bankruptcy Fraud Working Group; Cook County Region Organized Crime Organization; Financial Investigative Team, Milwaukee, Wisconsin; Madison, Wisconsin, SAR Review Team; Indiana Bank Fraud Working Group; Northern District of Indiana SAR Review Team; Southern District of Indiana SAR Review Team; FBI Louisville Financial Crime Task Force; U.S. Secret Service Louisville Electronic Crimes Task Force; Western District of Kentucky SAR Review Team; Eastern District of Kentucky SAR Review Team.
San Francisco Region	Fresno Mortgage Fraud Working Group for the Eastern District of California; Sacramento Mortgage Fraud Working Group for the Eastern District of California; Sacramento SAR Working Group; Orange County Financial Crimes Task Force-Central District of California; High Intensity Financial Crime Area Task Force; San Diego Financial Investigations and Border Crimes Task Force; Northern Nevada Financial Crimes Task Force.
Dallas Region	SAR Review Team for Northern District of Mississippi; SAR Review Team for Southern District of Mississippi; Oklahoma City Financial Crimes SAR Review Working Group; Austin SAR Review Working Group; Hurricane Harvey Working Group.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force; High Technology Crime Investigation Association; Cyberfraud Working Group; Council of the Inspectors General on Integrity and Efficiency Information Technology Subcommittee; National Cyber Investigative Joint Task Force; FBI Washington Field Office Cyber Task Force.

Other Key Priorities

In addition to the audits, evaluations, investigations, and other reviews conducted during the reporting period, our Office has emphasized other key initiatives. Specifically, in keeping with our Guiding Principles, we have focused on relations with partners and stakeholders, resource administration, and leadership and teamwork. A brief listing of some of our efforts in these areas follows.

Strengthening relations with partners and stakeholders.

- Communicated with the FDIC Chairman, FDIC Director, other FDIC Board Members, Chief Financial Officer, and other senior FDIC officials through the IG's and senior OIG leadership's regularly scheduled meetings with them and through other forums.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- Coordinated with the FDIC Director, in his capacity as Chairman of the FDIC Audit Committee, to provide status briefings and present the results of completed audits, evaluations, and related matters for his and other Committee members' consideration. Presented the results of OIG audits, evaluations, and other reviews at monthly Audit Committee meetings.
- Coordinated with DOJ and U.S. Attorneys' Offices throughout the country in the issuance of press releases announcing results of cases with FDIC OIG involvement and routinely informed the Chairman and FDIC Director of such releases.
- Attended FDIC Board Meetings and certain other senior-level management meetings to monitor or discuss emerging risks at the Corporation and tailor OIG work accordingly.
- Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our semiannual report to the Congress; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the FDIC's Office of Legislative Affairs on any Congressional correspondence pertaining to the OIG.
- Briefed Majority and Minority Staff of the House Committee on Financial Services on the FDIC OIG's assessment of the Top Management and Performance Challenges facing the FDIC, other audit work, and recent case highlights. Also briefed a House Appropriations Committee staff member on our 2020 budget request.

- Maintained the OIG Hotline to field complaints and other inquiries from the public and other stakeholders. The OIG's Whistleblower Protection Coordinator also helped educate FDIC employees who had made or were contemplating making a protected disclosure as to their rights and remedies against retaliation for such protected disclosures.
- Supported the IG community by attending monthly Council of the Inspectors General on Integrity and Efficiency (CIGIE) meetings and other meetings, such as those of the CIGIE Audit Committee, IT Committee, Investigations Committee, Professional Development Committee, Legislative Committee, Assistant Inspectors General for Investigations, Council of Counsels to the IGs, and Federal Audit Executive Council; responding to multiple requests for information on IG community issues of common concern; and commenting on various legislative matters through CIGIE's Legislative Committee.
- Presented a seminar to all OIG staff on the history of the IG Act of 1978 and its evolution over the 40 years since its passage.
- Participated on CIGFO, as established by the Dodd-Frank Act, and coordinated with the IGs on that Council. This Council facilitates sharing of information among CIGFO member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight. Contributed to CIGFO's joint assignment on the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments.
- Coordinated with the Government Accountability Office on ongoing efforts related to the annual financial statement audit of the FDIC and the FDIC's Annual Report, including with respect to the Top Management and Performance Challenges Facing the FDIC.
- Coordinated with the Office of Management and Budget to address budget matters of interest.
- Worked closely with representatives of the DOJ, including the Main Justice Department, FBI, and U.S. Attorneys' Offices, to coordinate our criminal investigative work and pursue matters of mutual interest. Joined law enforcement partners in numerous financial, mortgage, and cyber fraud-related working groups nationwide.

- Promoted transparency to keep the American public informed through three main means: the FDIC OIG Website to include, for example, summaries of completed work, listings of ongoing work, and information on unimplemented recommendations; Twitter communications to immediately disseminate news of report and press release issuances and other news of note; and participation in the IG community's oversight.gov Website, which enables users to access, sort, and search thousands of previously issued IG reports and other oversight areas of interest.

- Developed a new outreach brochure explaining the mission and role of the FDIC OIG for both internal FDIC and external stakeholders to better familiarize them with the work of the OIG and the various avenues for contacting the OIG with questions or to report waste, fraud, and abuse involving FDIC programs, operations, or supervised institutions.

Administering resources prudently, safely, securely, and efficiently.

- Continued efforts by the OIG's Office of Information Technology to coordinate a strategic approach to facilitate the integration of technology in OIG processes. This group is responsible for the OIG's enterprise architecture, and IT governance and related policies and procedures. Successfully migrated OIG email to the Cloud as a tenant segregated from the FDIC to ensure emails remain separate and independent from the agency. Also carried out a technology refresh, including migrating technology from out-of-date and unsupported hardware to new, faster hardware.
- Prepared a budget justification document for the Office of Management and Budget and for the FDIC OIG's Senate and House Appropriations Committees to support a fiscal year 2020 budget of $43 million to fund 144 authorized positions.
- Conducted training for OIG staff on Phishing and how to avoid becoming a victim. Supplemented training with additional communications to staff regarding information security during the reporting period.
- Took steps to coordinate with FDIC officials on Emergency Preparedness for the OIG, including plans for emergency notifications and continuity of operations in the event of unforeseen circumstances.

- Relied on the OIG's General Counsel's Office to ensure our Office complied with legal and ethical standards, rules, principles, and guidelines; provide legal advice and counsel to teams conducting audits and evaluations; and support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- Continued to review and update a number of OIG internal policies related to audit, evaluation, investigation, management operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the office.
- Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included an Attorney Advisor, an IT Specialist, a Digital Investigative Analyst, and a Human Resources Specialist.
- Oversaw contracts to qualified firms to provide audit, evaluation, IT, and other services to the OIG to provide support and enhance the quality of our work and the breadth of our expertise as we conduct audits, evaluations, and investigations, and to complement other OIG functions and closely monitored contractor performance.
- Continued to closely monitor, track, and control OIG spending, with particular attention to expenses involved in procuring equipment, software, and services to improve the OIG's IT environment.
- Procured a new server for the OIG's Electronic Crimes Unit, removed unnecessary digital data, revised procedures, and retired outdated equipment to better leverage ECU capabilities and serve Office needs.

Exercising leadership skills and promoting teamwork.

- Promoted two Special Agents from the Office of Investigations to serve as Special Agents in Charge of two Regional Offices in Atlanta and Kansas City.
- Continued biweekly OIG senior leadership meetings to affirm the OIG's unified commitment to the FDIC OIG mission and to strengthen working relationships and coordination among all FDIC OIG offices.

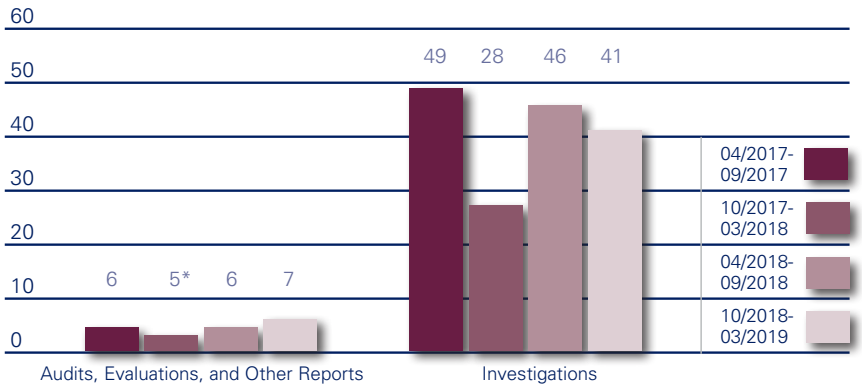
- Developed strategic plans for individual OIG offices, aligned with the OIG's Guiding Principles, and taking into consideration current resources, skills, accomplishments, challenges, and goals for the future. These individual plans form the basis for budget requests, promote further understanding of component offices, and help ensure that office-wide efforts in pursuit of the OIG mission are efficient, effective, and economical.
- Supported efforts of the IG Advisory Council, a cross-cutting group of OIG staff whose mission is to provide leadership toward "One OIG" by promoting collaboration and innovation.
- Leveraged the OIG's Data Analytics capabilities to improve the overall efficiency and effectiveness of the OIG's audit and evaluation assignments; identify and reduce fraud, waste, and abuse; and facilitate OIG decision-making.
- Kept OIG staff informed of Office priorities and key activities through regular meetings among staff and management, bi-weekly updates from senior management meetings, and issuance of OIG newsletters.
- Offered multiple POWER Lunch and Learn sessions to all OIG staff to enhance their knowledge of such areas as the 116th Congress, the Dark Web, and Protecting the Nation's Critical Infrastructure.
- Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
- Carried out monthly coordination meetings for audit, evaluation, and investigation leadership to better communicate, coordinate, and maximize the effectiveness of ongoing work.
- Acknowledged individual and group accomplishments through an ongoing awards and recognition program.
- Continued to support members of the OIG pursuing professional training and certifications or attending graduate banking school programs to enhance the OIG staff members' expertise and knowledge.
- Sponsored several training sessions on reporting for all audit and evaluation staff, including a 2-day session on Developing the Message Through Critical Thinking and additional training on Excel functions.

- Fostered a sense of teamwork and mutual respect through various activities of the OIG's Diversity and Inclusiveness (D&I) Working Group. These included developing a D&I charter, hosting an IG panel on D&I, encouraging all OIG staff to take advantage of FDIC Corporate University's Diversity 101 course offering, and sponsoring a diversity-themed lunch for all staff. Also added a new D&I page on the OIG's intranet.
- Responded to suggestions received through the OIG Solutions Box, which provides all staff a mechanism to suggest positive improvements to the workplace.

Cumulative Results (2-year period)

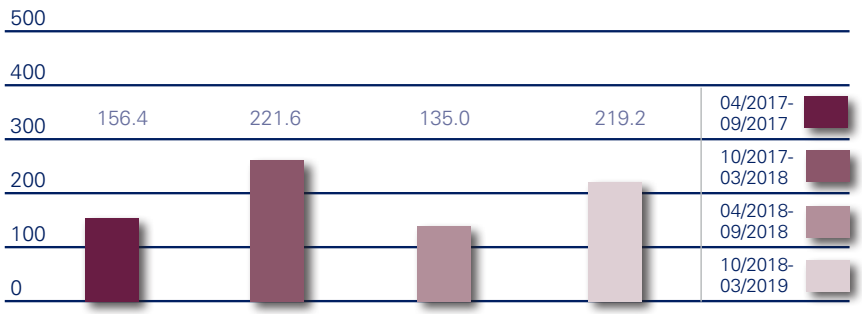
Nonmonetary Recommendations	
April 2017 – September 2017	36
October 2017 – March 2018	33
April 2018 – September 2018	29
October 2018 – March 2019	24

Products Issued and Investigations Closed



*Does not include two Failed Bank Reviews.

Fines, Restitution, and Monetary Recoveries Resulting from OIG Investigations ($ millions)



Reporting Requirements

Index of Reporting Requirements - Inspector General Act of 1978, as amended

Reporting Requirements	Page
Section 4(a)(2) Review of legislation and regulations.	42
Section 5(a)(1) Significant problems, abuses, and deficiencies.	6-17
Section 5(a)(2) Recommendations with respect to significant problems, abuses, and deficiencies.	6-17
Section 5(a)(3) Recommendations described in previous semiannual reports on which corrective action has not been completed.	43
Section 5(a)(4) Matters referred to prosecutive authorities.	53
Section 5(a)(5) Summary of each report made to the head of the establishment regarding information or assistance refused or not provided.	53
Section 5(a)(6) Listing of audit, inspection, and evaluation reports by subject matter with monetary benefits.	50
Section 5(a)(7) Summary of particularly significant reports.	6-17
Section 5(a)(8): Statistical table showing the total number of audit reports and the total dollar value of questioned costs.	51
Section 5(a)(9) Statistical table showing the total number of audit reports and the total dollar value of recommendations that funds be put to better use.	52
Section 5(a)(10) Summary of each audit, inspection, and evaluation report issued before the commencement of the reporting period for which	
• no management decision has been made by the end of the reporting period	52
• no establishment comment was received within 60 days of providing the report to management	52
• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	44-49
Section 5(a)(11) Significant revised management decisions during the current reporting period.	52

Reporting Requirements (continued)	Page
Section 5(a)(12) Significant management decisions with which the OIG disagreed.	53
Section 5(a)(14, 15, 16) An appendix with the results of any peer review conducted by another OIG during the period or if no peer review was conducted, a statement identifying the last peer review conducted by another OIG.	56
Section 5(a)(17): Statistical tables showing, for the reporting period: • number of investigative reports issued • number of persons referred to the DOJ for criminal prosecution • number of persons referred to state and local prosecuting authorities for criminal prosecution • number of indictments and criminal Informations.	53
Section 5(a)(18) A description of metrics used for Section 5(a)17 information.	53
Section 5(a)(19) A report on each OIG investigation involving a senior government employee where allegations of misconduct were substantiated, including • the facts and circumstances of the investigation • the status and disposition of the matter, including if referred to the DOJ, the date of referral, and the date of DOJ declination, if applicable.	53
Section 5(a)(20) A detailed description of any instance of Whistleblower retaliation, including information about the official engaging in retaliation and what consequences the establishment imposed to hold the official responsible.	54
Section 5(a)(21) A detailed description of any attempt by the establishment to interfere with OIG independence, including with respect to budget constraints, resistance to oversight, or restrictions or delays involving access to information.	54
Section 5(a)(22) A detailed description of each OIG inspection, evaluation, and audit that is closed and was not disclosed to the public; and OIG investigation involving a senior government employee that is closed and was not disclosed to the public.	54

Appendix 1

Information Required by the Inspector General Act of 1978, as Amended

Review of Legislation and Regulations

The FDIC OIG's review of legislation and regulations during the past 6-month period involved continuing efforts to monitor and/or comment on enacted law or proposed legislative matters. In March 2019, Inspector General Lerner became Vice Chair of the CIGIE Legislation Committee. The FDIC OIG reviewed and provided input to the Legislation Committee on the CIGIE Legislative Priorities for the 116th Congress and H.R. 135, the *Federal Employee Antidiscrimination Act of 2019*.

With respect to the CIGIE Legislative Priorities, the IG community has a strong interest in several specific legislative proposals. The Legislation Committee has offered to provide technical assistance to advance related legislation in the following areas:

- Protecting cybersecurity vulnerability information.
- Testimonial subpoena authority.
- Reforming the Program Fraud Civil Remedies Act.
- Notification to Congress of decision to place an IG on paid or unpaid, non-duty status.
- Protection against reprisal for federal subgrantee employees.
- Statutory exclusion for felony fraud convicts to protect federal funds.
- Enhancing Lead IG oversight for Overseas Contingency Operations.
- Technical amendments to the Inspector General Reform Act of 2008.

Significant Recommendations from Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed

This table shows the corrective actions management has agreed to implement but has not completed, along with associated monetary amounts, as applicable. The information in this table is based on (1) information supplied by the FDIC's Risk Management and Internal Control (RMIC) branch, Division of Finance, and (2) the OIG's determination of when a recommendation can be closed. RMIC has categorized the status of these recommendations as follows:

Management Action in Process: (three recommendations from two reports)

Management is in the process of implementing the corrective action plan, which may include modifications to policies, procedures, systems or controls; issues involving monetary collection; and settlement negotiations in process.

Table I: Significant Recommendations from Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed

Report Number, Title, and Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action in Process		
AUD-18-001 **Audit of the FDIC's Information Security Program - 2017** October 25, 2017	6*	The FDIC will develop and integrate an enterprise security architecture into the corporate-wide enterprise architecture (EA) consistent with federal enterprise architecture requirements.
AUD-18-004 **The FDIC's Governance of Information Technology Initiatives** July 26, 2018	3*	The Chief Information Officer Organization (CIOO) has implemented an EA that is part of the FDIC's Information Technology (IT) Governance Framework and used to guide IT decision-making. Specifically, the governance component of the EA Program is implemented through the SEATAB Charter.
	7	As part of the CIOO's ongoing Enterprise IT Maturity Program, the CIOO will develop a workforce planning process that will ensure the identification and documentation of the IT resources and expertise needed to execute the FDIC's IT Strategic Plan.

*The OIG has not completed the evaluation of management's actions in response to the OIG's recommendation.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-16-001 **FDIC's Information Security Program – 2015** October 28, 2015	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct a performance audit to evaluate the effectiveness of the FDIC's information security program and practices. Overall, C&C concluded that the FDIC's information security program and practices were generally effective and noted several important improvements in the FDIC's information security program over the past year. However, C&C noted that the FDIC had not assessed whether Information Security Managers had requisite skills, training, and resources. Also, the FDIC had not always timely completed outsourced information service provider assessments or review of user access to FDIC systems. Other findings involved control areas of risk management and configuration management. The report contained six recommendations to improve the effectiveness of the FDIC's information security program controls and practices.	6	1	NA
AUD-17-001 **Audit of the FDIC's Information Security Program – 2016** November 2, 2016	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct a performance audit to evaluate the effectiveness of the FDIC's information security program and practices. C&C found that the FDIC had established a number of information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. However, C&C described security control weaknesses that impaired the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at elevated risk. C&C reported on 17 findings, of which 6 were identified during the current year FISMA audit and the remaining 11 were identified in prior OIG or Government Accountability Office reports. These weaknesses involved: strategic planning, vulnerability scanning, the Information Security Manager Program, configuration management, technology obsolescence, third-party software patching, multi-factor authentication, contingency planning, and service provider assessments. The report contained six new recommendations addressed to the Chief Information Officer to improve the effectiveness of the FDIC's information security program and practices.	6	1	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-17-007 **Controls over Separating Personnel's Access to Sensitive Information** September 18, 2017	The FDIC experienced a number of data breaches in late 2015 and early 2016 that involved employees who were exiting the Corporation. In response, the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs requested that the FDIC OIG examine issues related to the FDIC's policies governing departing employees' access to sensitive financial information. Our evaluation objective was to determine the extent to which the FDIC had established controls to mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel. While the FDIC had established and implemented various control activities, we found that there were weaknesses in the design of certain controls, Division and Office records liaisons were not always following procedures, and opportunities existed to strengthen the pre-exit clearance process. As designed, the program controls did not provide reasonable assurance that the pre-exit clearance process would timely or effectively identify unauthorized access to, or inappropriate removal and disclosure of, sensitive information by separating employees. We noted that separating contractor employees (contractors) may present greater risks than separating FDIC employees. We found several differences between the pre-exit clearance process for FDIC employees and contractors that increased risks related to protecting sensitive information when contractors separated. We also found that the FDIC was not consistently following its pre-exit clearance procedures with respect to separating contractors, and we identified several opportunities for strengthening the contractor pre-exit clearance process. The report contained 11 recommendations to provide the FDIC with greater assurance that its controls mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel.	11	2	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-18-001 **Audit of the FDIC's Information Security Program – 2017** October 25, 2017	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct an audit to evaluate the effectiveness of the FDIC's information security program and practices. The audit included a review of selected security controls related to three general support systems, one business application, and the FDIC's risk management activities pertaining to four outsourced information service providers. As part of its work, C&C developed responses to security related questions contained in the Department of Homeland Security's document, entitled FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V 1.0, dated April 17, 2017 (the IG FISMA Reporting Metrics). C&C's report describes security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. C&C reported a total of 19 findings, of which 14 were identified during the current year FISMA audit and the other 5 were identified in prior reports issued by the OIG or the Government Accountability Office. C&C's report contained 18 recommendations addressed to the FDIC's Chief Information Officer that were intended to improve the effectiveness of the FDIC's information security program and practices.	18	6	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
OIG-18-001 **The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches** April 16, 2018	The FDIC OIG conducted this review at the request of the former Chairman of the Senate Committee on Banking, Housing, and Urban Affairs. The former Committee Chairman asked that the FDIC OIG examine issues at the FDIC related to data security, incident reporting, and policies, as well as representations made by FDIC officials to Congress. During late 2015 and early 2016, the FDIC experienced eight information security incidents as departing employees improperly took sensitive information shortly before leaving the FDIC. Seven of the eight incidents involved personally identifiable information, including Social Security Numbers, and thus constituted breaches. In the eighth incident, the departing employee took highly sensitive components of resolution plans submitted by certain large systemically important financial institutions without authorization. The report contained 13 recommendations to address systemic issues associated with the FDIC's incident response and reporting, and interactions with Congress. We also discussed issues related to certain individuals' performance of their responsibilities during the timeframes under review.	13	1	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-18-004 **The FDIC's Governance of Information Technology Initiatives** July 26, 2018	Federal statutes and Office of Management and Budget policy require federal agencies to establish and implement fundamental components of IT governance. These components include IT strategic planning, which defines the overall direction and goals for the agency's IT program, and an enterprise architecture, which describes the agency's existing and target architecture and plan to achieve the target architecture. Our audit objective was to identify key challenges and risks that the FDIC faced with respect to the governance of its IT initiatives. We found that the FDIC faced a number of challenges and risks with respect to the governance of its IT initiatives. Specifically, the FDIC had not fully developed a strategy to migrate IT services and applications to the cloud or obtained the acceptance of key business stakeholders before taking steps to initiate cloud projects. In addition, the FDIC had not implemented an effective enterprise architecture to govern its IT decision-making or completed needed revisions to its IT governance processes to ensure sufficiently robust governance for all of its IT initiatives. The FDIC had also not fully integrated security within its IT governance framework or acquired the resources and expertise needed to support the adoption of cloud solutions. Further, the FDIC did not use complete cost information or fully consider intangible benefits when evaluating cloud solutions. The FDIC took a number of actions to strengthen its IT governance during and after our audit. The report included eight recommendations to improve upon these efforts.	8	1	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-18-004 **Forward-Looking Supervision** August 8, 2018	The FDIC adopted a risk-focused supervision program in 1997, and in 2011, the FDIC implemented a Forward-Looking Supervisory initiative as part of its risk-focused supervision program. The goals of this supervisory approach are to identify and assess risk before it impacts a financial institution's financial condition and to ensure early risk mitigation. Our evaluation objective was to determine whether the Forward-Looking Supervision approach achieved its outcomes--the Division of Risk Management Supervision pursued supervisory action upon identifying risks and the financial institutions implemented corrective measures. We found that the FDIC did not have a comprehensive policy guidance document on Forward-Looking Supervision. In addition, we identified instances in which examiners did not always document certain Forward-Looking Supervision concepts consistent with examiner guidance, when planning an examination and when reporting examination results. The report included four recommendations to improve implementation of Forward-Looking Supervision.	4	2	NA

Table III: Audit and Evaluation Reports Issued by Subject Area

Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	**Title**	**Total**	**Unsupported**	
Information Technology and Cybersecurity				
AUD-19-001 October 25, 2018	*The FDIC's Information Security Program - 2018*			
AUD-19-002 December 4, 2018	*Controls Over System Interconnections with Outside Organizations*			
AUD-19-003 December 10, 2018	*Payments to Pragmatics, Inc.*	$47,489	$7,510	
AUD-19-004 January 16, 2019	*Security Configuration Management of the Windows Server Operating System*	$ 1,080		
Totals for the Period		**$48,569**	**$7,510**	**$0**

Other products issued:

- *Loan Sample Methodology of Examinations*
PAE Memorandum 19-001
February 4, 2019
- *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation*
February 14, 2019
- *Analysis of FDIC Purchase Card and Convenience Check Transactions*
ITC Memorandum 19-001
March 19, 2019

Table IV: Audit and Evaluation Reports Issued with Questioned Costs

	Number	Questioned Costs	
		Total	Unsupported
A. For which no management decision has been made by the commencement of the reporting period.	0	$0	$0
B. Which were issued during the reporting period.	2	$48,569	$7,510
Subtotals of A & B	**2**	**$48,569**	**$7,510**
C. For which a management decision was made during the reporting period.	1	$1,080	$0
(i) dollar value of disallowed costs.	0	$1,080	$0
(ii) dollar value of costs not disallowed.	0	$0	$0
D. For which no management decision has been made by the end of the reporting period.	1	$47,489	$7,510
Reports for which no management decision was made within 6 months of issuance.	0	$0	$0

Table V: Audit and Evaluation Reports Issued with Recommendations for Better Use of Funds

	Number	Dollar Value
A. For which no management decision has been made by the commencement of the reporting period.	0	$0
B. Which were issued during the reporting period.	0	$0
Subtotals of A & B	**0**	**$0**
C. For which a management decision was made during the reporting period.	0	$0
(i) dollar value of recommendations that were agreed to by management.	0	$0
- based on proposed management action.	0	$0
- based on proposed legislative action.	0	$0
(ii) dollar value of recommendations that were not agreed to by management.	0	$0
D. For which no management decision has been made by the end of the reporting period.	0	$0
Reports for which no management decision was made within 6 months of issuance.	0	$0

Table VI: Status of OIG Recommendations Without Management Decisions

During this reporting period, there were no recommendations more than 6 months old without management decisions.

Table VII: Status of OIG Reports Without Comments

During this reporting period, there were no reports where comments were received after 60 days of providing the report to management.

Table VIII: Significant Revised Management Decisions

During this reporting period, there were no significant revised management decisions.

Table IX: Significant Management Decisions with Which the OIG Disagreed

During this reporting period, there were no significant management decisions with which the OIG disagreed.

Table X: Instances Where Information Was Refused

During this reporting period, there were no instances where information was refused.

Table XI: Investigative Statistical Information

Number of Investigative Reports Issued	41
Number of Persons Referred to the Department of Justice for Criminal Prosecution	37
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	5
Number of Indictments and Criminal Informations	36

Description of the metrics used for the above information: Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 37 referrals to the Department of Justice, the total represents 29 individuals and 8 business entities. Four individuals and one business entity were referred to state and local prosecutors. Our total indictments and criminal informations includes indictments, informations, and superseding indictments, as applicable.

Table XII: OIG Investigations Involving Senior Government Employees Where Allegations of Misconduct Were Substantiated

During this reporting period, there were no investigations involving senior government employees where allegations of misconduct were substantiated.

Table XIII: Instances of Whistleblower Retaliation

During this reporting period, there were no instances of Whistleblower retaliation.

Table XIV: Instances of Agency Interference with OIG Independence

During this reporting period, there were no attempts to interfere with OIG independence.

Table XV: OIG Inspections, Evaluations, and Audits That Were Closed and Not Disclosed to the Public; and Investigations Involving Senior Government Employees That Were Closed and Not Disclosed to the Public

During this reporting period, there were no evaluations or audits closed and not disclosed to the public. There were no investigations involving senior government employees that were closed and not disclosed to the public.

Appendix 2

Information on Failure Review Activity (required by the Dodd-Frank Wall Street Reform and Consumer Protection Act)

FDIC OIG Review Activity for the Period October 1, 2018 through March 31, 2019 (for failures that occur on or after January 1, 2014 causing losses to the Deposit Insurance Fund of less than $50 million)

When the Deposit Insurance Fund incurs a loss under $50 million, Section 38(k) of the Federal Deposit Insurance Act requires the Inspector General of the appropriate federal banking agency to determine the grounds upon which the state or federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an in-depth review of the loss.

The FDIC OIG issued its most recent Failed Bank Review on February 14, 2018, that of Farmers and Merchants Bank, Argonia, Kansas, which failed on October 13, 2017. There have been no failures of FDIC-supervised financial institutions since that time. The OIG has no Failed Bank Reviews in process or pending.

Appendix 3

Peer Review Activity

Federal Inspectors General are required to engage in peer review processes related to both their audit and investigative operations. The FDIC OIG is reporting the following information related to its peer review activities. These activities cover our most recent roles as both the reviewed and the reviewing OIG and relate to both audit and investigative peer reviews.

Audit Peer Reviews

On the audit side, on a 3-year cycle, peer reviews are conducted of an OIG audit organization's system of quality control in accordance with the *CIGIE Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General*, based on requirements in the Government Auditing Standards (Yellow Book). Federal audit organizations can receive a rating of pass, pass with deficiencies, or fail.

Definition of Audit Peer Review Ratings

Pass: The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

Pass with Deficiencies: The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects with the exception of a certain deficiency or deficiencies that are described in the report.

Fail: The review team has identified significant deficiencies and concludes that the system of quality control for the audit organization is not suitably designed to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects or the audit organization has not complied with its system of quality control to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

- The U.S. Railroad Retirement Board OIG conducted a peer review of the FDIC OIG's audit organization and issued its system review report on November 14, 2016. In the Railroad Retirement Board OIG's opinion, the system of quality control for our audit organization in effect for the year ending March 31, 2016, had been suitably designed and complied with to provide our office with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. We received a peer review rating of pass.

- The report's accompanying letter of comment contained recommendations that, while not affecting the overall opinion, were designed to further strengthen the system of quality control in the FDIC OIG Office of Audits and Evaluations.

This peer review report is posted on our Website at www.fdicoig.gov.

Note: Our next semiannual report will include the results of the first peer review of our Evaluations function, conducted by the OIG for the Board of Governors of the Federal Reserve System and Bureau of Consumer Financial Protection.

FDIC OIG Peer Review of the Tennessee Valley Authority OIG

The FDIC OIG completed a peer review of the system of quality control for the audit organization of the Tennessee Valley Authority (TVA) OIG, and we issued our final report to that OIG on May 16, 2017. We reported that in our opinion, the system of quality control for the audit organization of the TVA OIG, in effect for the 12 months ended September 30, 2016, had been suitably designed and complied with to provide the TVA OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. The TVA OIG received a peer review rating of pass.

We also issued a letter of comment to the TVA OIG that set forth findings and recommendations that were not considered to be of sufficient significance to affect our overall opinion.

TVA OIG posted the peer review report on its Website at http://oig.tva.gov/peer_reports.html.

The FDIC OIG recently completed a peer review of the audit organization of the Special Inspector General for Afghanistan Reconstruction. We will report those results in our next semiannual report.

Investigative Peer Reviews

Quality assessment peer reviews of investigative operations are conducted on a 3-year cycle as well. Such reviews result in a determination that an organization is "in compliance" or "not in compliance" with relevant standards. These standards are based on *Quality Standards for Investigations* and applicable Attorney General Guidelines. For our office, applicable Attorney General Guidelines include the Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority (2003), Attorney General Guidelines for Domestic Federal Bureau of Investigation Operations (2008), and Attorney General Guidelines Regarding the Use of Confidential Informants (2002).

- The Department of the Treasury OIG conducted a peer review of our investigative function and issued its final report on the quality assessment review of the investigative operations of the FDIC OIG on February 1, 2016. The Department of the Treasury OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of the FDIC OIG in effect for the year ending December 31, 2015, was in compliance with quality standards established by the CIGIE and the applicable Attorney General guidelines. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations.

The Department of the Treasury OIG recently concluded another peer review of our investigative function, and we will report the results of this more recent review in our next semiannual report.

- The FDIC OIG conducted a peer review of the investigative function of the Small Business Administration (SBA) OIG. We issued our final report to SBA OIG on December 19, 2017. We reported that, in our opinion, the system of internal safeguards and management procedures for the investigative function of the SBA OIG in effect for the period ending August 31, 2017, was in compliance with the quality standards established by CIGIE and other applicable guidelines and statutes.

Congratulations and Farewell

The following staff members retired from the FDIC OIG during the reporting period. We appreciate their many contributions to the FDIC over the years, congratulate them on their Federal service, and wish them well in future endeavors.

Mike Dann
Special Agent, Office of Investigations, Electronic Crimes Unit.

Jason Moran
Special Agent in Charge, Office of Investigations, Atlanta Region.

Donald DeVille
Senior Audit Specialist, Office of Program Audits and Evaluations.

****

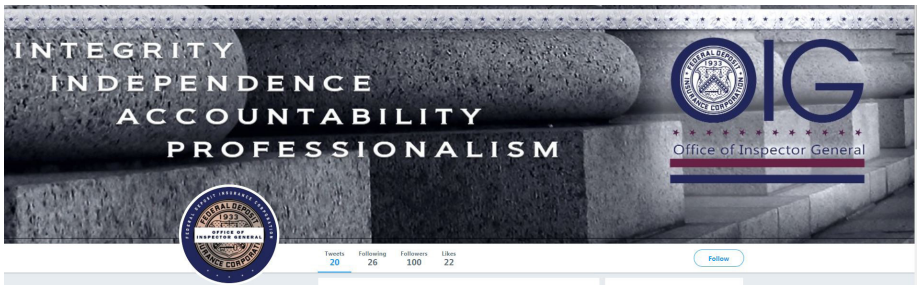
Fred Gibson
Deputy Inspector General

During the reporting period, Fred Gibson left the FDIC OIG to become the Deputy IG at the Federal Reserve Board OIG. Fred served as the FDIC Acting Inspector General for 3½ years during challenging times in the banking and financial services industry. Previously, Fred was central to establishing the FDIC OIG's authorities for criminal investigations, including bank fraud, money laundering, obstruction of bank examinations, and concealment of assets. Fred also brought his banking law experience to bear on numerous audits and evaluations. The FDIC OIG wishes Fred continued success in his new role.

Keep Informed

Learn more about the FDIC OIG.
Visit our Website: www.fdicoig.gov

Follow us on Twitter: @FDIC_OIG



View the work of 73 Federal OIGs on the IG Community's Website

OVERSIGHT.GOV
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

Federal Deposit Insurance Corporation
Office of Inspector General
3501 Fairfax Drive
Arlington, VA 22226

OIG HOTLINE

The Office of Inspector General Hotline is a convenient mechanism employees, contractors, and others can use to report instances of suspected fraud, waste, abuse, and mismanagement within the FDIC and its contractor operations. Instructions for contacting the Hotline and an on-line form can be found at www.fdicoig.gov.

Whistleblowers can contact the OIG's Whistleblower Protection Coordinator through the Hotline by indicating: Attention: Whistleblower Protection Coordinator.

DESIGN: FDIC/DOA/CSB/GRAPHIC DESIGN AND PRINTING UNIT

FDIC-030-2019